International Journal of Technological Exploration and Learning (IJTEL)
ISSN: 2319-2135
Volume 2 Issue 5 (October 2013)

# Anomaly Based Intrusion Detection using Feature Relevance and Negative Selection Algorithm

Jothi Lakshmi U
Assistant Professor,
Department of Information Technology,
PITAM,Chennai,India

***Abstract*— With the increase in the use of internet, the job of malicious people has been made easy to exploit vulnerabilities in existing system. Intrusion Detection System (IDS) plays a major role in computer/network security in recognizing such malicious activity called intrusion. IDSs' quick and correct detection of unknown intrusions help in reducing damage/loss to the sensitive information. IDS with such quality need to be encouraged. An IDS must analyse a different set of attributes to decide upon a monitored information as normal or abnormal. This becomes a time consuming task if the number of attributes to be analysed are more. Hence this becomes a barrier for fast detection. This paper proposes and implements an intrusion detection approach that breaks this barrier and helps in correct detection of novel attacks. This is achieved by using significant feature set extracted from KDDcup1999 dataset and Negative Selection Algorithm (NSA) an Artificial Immune System concept.**

***Keywords-Intrusion Detection; Feature Relevance; Negative Selection; Anomaly Based Intrusion Detection.***

## I. Introduction

Nowadays attackers have become more sophisticated that any sector is vulnerable to threats and attacks in spite of advanced security measures. The notion of intrusion detection followed by Intrusion Detection System (IDS) came into picture when the threat and attack has become a guaranteed one. IDS is the process of monitoring events for facts of security policy violations or attempt. Intrusion occurs at any point of time and it is unpredictable. So an IDS need to be alert all the time monitoring and analysing the data it come across. An IDS is categorised into two – Data source based and Analysis method based. Data source is again classified into two, 1) Host based and 2) Network based. Analysis based is again classified into two, 1) misuse based and 2) anomaly based. Misuse looks for attack signatures of known attacks while anomaly is based on profile of normality. A significant deviation from this profile of reference indicates a potential threat. Misuse based holds the advantage of accurate detection of attack whereas Anomaly based holds the advantage of detecting unknown attacks also called as zero-day attacks. Most traditional intrusion detection systems (IDS) take either a network- or a host-based approach to recognize and detect attacks. In either case, these products look for attack signatures, specific patterns that usually indicate malicious or suspicious intent. Network- based IDS looks for network traffic pattern and in host-based IDS looks for patterns of system calls, log files etc. IDS recognize various types of attack that are categorised under four classes namely – Denial-of-service, Probe, User-to-Root, Root-to-User. The first two are called fast attacks and next two are slow attacks. Fast and slow here means, the time take taken by the attacker to exploit the vulnerability. Hybrid models of IDS are preferred much especially - combination of misuse and anomaly – for better performance. In general IDS analyzes large set of attributes which leads to slow detection. If the attribute under analysis contributes less in attack detection then it may lead to less accurate results .If signature based-IDS is considered, updating the signature store is often needed. Otherwise it suffers from false positives. This also leads to the reduced accuracy and slow detection issue. In Anomaly based IDS false alarms will be high that suppress normal activity if automatic response is incorporated in the system.

In this proposal, an intrusion detection approach for anomaly based network intrusion detection system (NIDS) that exhibits Artificial Immune System (AIS) mechanism called Negative Selection Algorithm [17] is presented. The motivation is to bring up an approach that supports fast and accurate detection of anomalies. The experiment is done considering features in KDDcup 99 dataset.

The rest of this paper is organized as follows. In Section II, we discuss some related work in the literature on IDS using Artificial Immune System and feature selection approaches in IDS. Negative Selection mechanism in AIS and importance of feature selection in IDS is also discussed. Section III gives the detail of system design which includes proposed approach.

Section IV gives result and evaluation, followed by conclusion and foreseeable enhancement in Section V.

## II. Related Works

### *A. IDS*

IDS in a very simple form is a process of monitoring events for facts of security policy violations or attempt. IDS is of different types. Table 1 provides a brief description on IDS types. Most of the real time system comes is combination of these types [26-27, 32-33]. Many available IDS products like Snort, Cisco, etc support signature-based analysis method [33]. Though signature based cannot recognize new or unknown attacks. Different approaches are applied to IDS namely, Datamining, Fuzzy Logic, Genetic Algorithm, Artificial Neural Network, Artificial Immune System, Swarm Intelligence. Many of IDS model are hybrid ones combining any of above mentioned approach.

### 1) *Anomaly Based IDS*

Anomaly detection or change detection is an analysis method in IDS for finding the deviation from normality. In this an IDS gets trained in the normal environment. Then maintains a normal profile and compares it with the incoming real data. If a remarkable deviation is found then an abnormality is identified. Remarkable here means crossing a preset threshold value. One important advantage of Anomaly Based IDS over Signature based is it has the capability of recognising unknown attacks. Problem with this method is the

1. Large number of false alarms,

2. Profiling complete / exact normal behaviour impossible.

TABLE I. TYPES OF IDS IN SHORT DESCRIPTION

| IDS types | Host Based | Network Based |
|---|---|---|
| **Signature Based** | Data collected is from a single host – audit logs or system calls. Signatures are extracted from this collected data when any attack is identified. | Network data is monitored and collected. Signatures are extracted from this collected data when any attack is identified. |
| **Anomaly Based** | Data collected is from a single host. Normal activities are profiled in an attack free environment | Network data is monitored and collected. Normal activities are profiled in an attack free environment |

Evaluation of any type of IDS (Signature or Anomaly based)

is made using following two main measures[21],

1. detection rate (DR)
2. false positive rates (FPR)

$$DR = DA/T \quad (1)$$

where DA is number of truly detected attacks and T is total number of attacks identified.

$$FPR = F/N \quad (2)$$

where F is number of false alarms and N is total number of normal connections.

## B. *Feature Selection in IDS*

Dimensionality reduction is a major issue in IDS. Increase in dimension increases computation complexities. The IDS's benchmark dataset collected by MIT Lincoln Lab is represented using 41 features in KDDcup1999 dataset. [www5, 5] provides more details about these features. 41 features is truly a higher dimension. In this, not all the 41 features are relevant pertaining to any specific attack detection. But any one particular feature might play an important role in detecting a attack. So there is a necessity to select the relevant feature among these 41 specific to attacks.

Feature Selection is a method of identifying most relevant features from a set of given features. Methods [22] for feature selection have been essentially divided into two categories: filter method and wrapper method. Each has its own advantages and disadvantages. Feature subset selection is a possible means of improving the performance intrusion detection system. Support Vector Machine (SVM), Rough Set Theory (RST), Information Gain (IG), Genetic Algorithm (GA) are few among various approaches that support feature selection.

In [1,2,5,7,8,12,18,19,21,22 - 24], the importance of feature selection is taken into account mainly for improving detection rate and detection accuracy in addition to reducing computation time and data size.

Yang Li, et.al [22] have given experimental results of performance improvement by selecting relevant features. In that a Modified Random Mutation Hill Climbing algorithm is used for search strategy and Modified SVM is used for evaluation and nine features are selected as most relevant ones.

According to the survey that has been carried out for the project work, a total of ten features are more relevant in discriminating normal from attacks out of 41 features mentioned in KDDcup99 dataset.

AIS based mechanisms for IDS

Artificial Immune System [3, 4, 6, 9, 11, 15 - 17] is an insight from immunology – a science that deals with human, plant, vertebrate immune system (IS). *IS* is a complex system that works through out the life time of any living being. It is a system that is complex, distributed, adaptive, and robust that provides innate immunity, and also has the ability to learn the environment and adapt to it overtime.

Few mechanism of IS are applied to IDS. Negative Selection is one main mechanism; applied to IDS way back in 1999 to a system named LISYS (Lightweight Immune SYStem).This system is the implementation of ARTIS (ARTificial Immune System) framework proposed by Steven A. Hofmeyr [17]. Other popular mechanisms that are in use in AIS for IDS are Clonal Selection Algorithm, Dendritic Cell Algorithm and immune network theory. Clonal Selection and Negative Selection provide adaptive immunity to the system whereas DCA provide innate immunity. In [15], Negative Selection - its application to virus detection, Clonal Selection Immune networks are discussed in detail. The following discussion upon AIS is restricted to Negative Selection Algorithm as the proposed approach uses it. AIS simply mimics IDS functions. Thus AIS based IDS researches have raised remarkably from late 90's to till date.

### 1) *Negative Selection Algorithm*

Fig. 1 shows a general model of AIS based architecture for Anomaly based IDS. This model incorporates Negative Selection Algorithm (NSA) that is devised from Negative Selection Mechanism. NSA is one among many learning mechanism derived from IS.

Learning mechanism of NSA is on the basis of self/ nonself discrimination based on one class classification. In this all self data are identified initially. Non self detector (antibody) generation is based on this self data. In short, detectors (antibodies) are randomly generated and compared with self data. If a match is found then that detector is disqualified of being a detector. Else it is stored in a detector set. These detector set helps in identifying unknown attacks.

The real data is then compared with this detector set, if a match is found then that data is identified as nonself one and removed from the system. Fig. 2 shows self/non-self discrimination mechanism of NSA devised by Steven A.Hofmeyr et.al in 1999. Many of AIS based IDS uses NSA because it is a simple mechanism and best suited for anomaly detection.

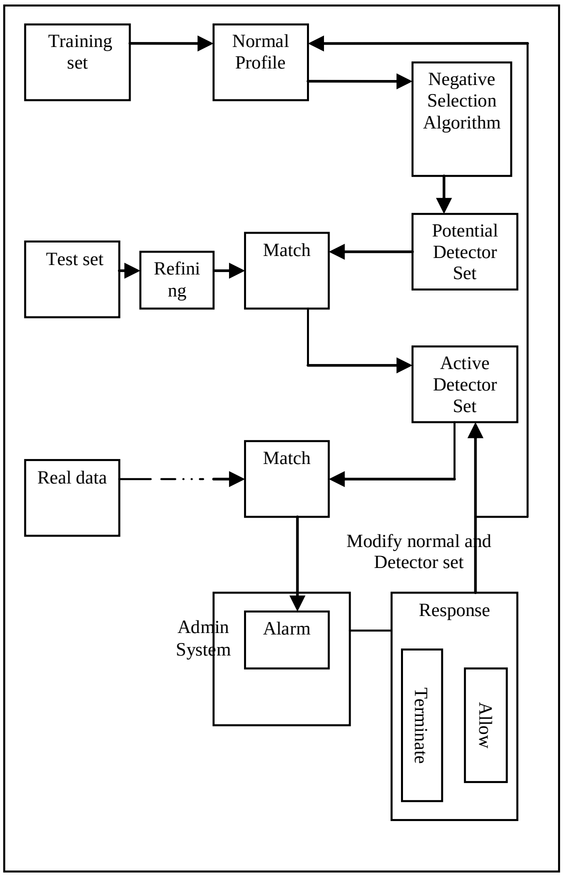

Fig. 1: Abstract model for AIS based IDS incorporating NSA

Other issues are scaling problem, detecting and filling holes, and detector coverage. Feng Gu et.al have concluded with this point in [4] by experimenting NSA with KDDcup 1999 dataset. Many of AIS based IDS (eg: ARTIS[15], EVOLUSIR [3] ) used DARPA/MIT Lincoln Laboratory off-line intrusion detection evaluation data set which is expressed using only six attribute. Shelly Xiaonan Wu's review report [21] points out NSA s' performance reduces with higher dimension data. The same indication is given by F.Gu in [4].

Taking this as a seed, this work concentrates in identifying a small set of features that has positive impact on attack discrimination and that supports NSA.

## III. SYSTEM DESIGN

The scope of this project work is to identify the most significant features relevant for intrusion detection from KDDCup1999 dataset and to utilize it to improve the Detection Rate, Accuracy and False Positive rate of Anomaly based intrusion detection technique using Negative selection Algorithm.

### A. PROPOSED APPROACH

In this proposed approach, the advantage of significant feature set and negative selection algorithm (NSA) have been utilised to provide good attack detection rate of novel attack and accuracy.

To overcome the dimensionality problem of NSA a modification is made in the generation of potential detectors through reducing the feature set based on the significance of the feature in attack discrimination. It has four different but interrelated steps that lead this approach to that improved detection rate. The steps are as follows,

*Step 1*: Data processing of KDD cup99 dataset,
*Step 2*: Generation of normal profile using processed data
*Step 3*: Detector Generation
*3.a*: Extract normal data instance based on feature subset – specific to attack detection
*3.b:* Generate potential anomaly detector sets from extracted normal connection profile
*3.c:* Generate active detector sets from potential detector sets
*Step 4:* Evaluate active detectors using real time data set.

The following section discusses each step in detail:

#### 1) *Data processing*

It is the method of moulding the raw input data into a form that is understandable by the algorithm to which it is applied. Two main steps related to data processing in the proposal are as follows,

- *Identify relevant feature set from the given dataset*
- *Representing Data Instances*

#### 2) Identify relevant feature set from the given dataset

In this step the irrelevant attributes are identified and eliminated from the dataset. For this purpose a survey on recent experiments each applying different techniques for identifying relevant features contributing in attack detection has been done. All these experiment is done upon KDD cup99 dataset.

These marked features are then tested for their contribution in discriminating an attack by applying a classification algorithm called C4.5 on these features. The scores of C4.5 is used for checking the significance of the identified feature set. Score here means the posterior probability of the positive class. Positive class here means the values of the class attribute (normal, Neptune, smurf.) in the KDD set. The result obtained is then compared with the scores of C4.5 with all 41 features in the dataset. From this survey it has been concluded that, features 1, 3, 5, 6, 23, 24, 25, 32, 33, and 35 are most relevant features [25].

#### 3) *Representing Data Instances*

In this step the data instances are expressed in algorithm understandable format. This is also called as encoding of data. In the proposed approach, data instances will be represented in a binary string format. The reason behind this is it is easy to represent and manage. The method of encoding is as follows:

The selected ten features are considered for each record. Among these ten features, all are continuous except service which is discrete. It has sixty six different values in training set. To convert this feature into binary, a simple method is followed. That is, each feature is assigned a number starting from 1 to 66. Floating point values are converted into integer value. Later it is converted to binary value. An example showing the method of encoding is given in APPENDIX 1.

### B. Normal Connection Profile (NCP) Generation

The identified feature set is then used for the normal connection profiling, from which potential detectors are identified and stored. KDD cup99 dataset's flaw in terms of redundant data will reflect in normal connection profiling. So before profiling redundant data will be removed as it is very important for perfect profiling of normal data and also reduces the profile size.

As KDD dataset is a labelled dataset, each instance is named as Normal or by specific attack names. For NCP purpose only the normal data need to be considered. The normal data alone are extracted from the dataset by making use of the component called Rule-Based Selection that is available in Tanagra tool. The extracted data is then encoded using the method that is mentioned in the above section.

### C. Detector Generation

In this step different sets of potential detectors are derived from the normal profile using NSA. From this Potential Detector Set (PDS), Active Detector Set (ADS) are generated. The flow of this process is given in Figure 5.2.

In this the terminating condition is number of preserved potential detectors. This is user defined say 200. Various matching rule for strings are found in literature, in that two important type of matching rule for binary encoding are rcb (r-contiguous bit match) and r-chunk [25].

The matching function used here works as follows and it is similar to rcb.

If, Random String (RS) = 1101010010 and Normal String (NS) = 0111110101101010010010110110011

then the RS is considered as a pattern P. Pattern P is then searched in the NS,

NS 011111010**1101010010**010110110011
RS **1101010010**

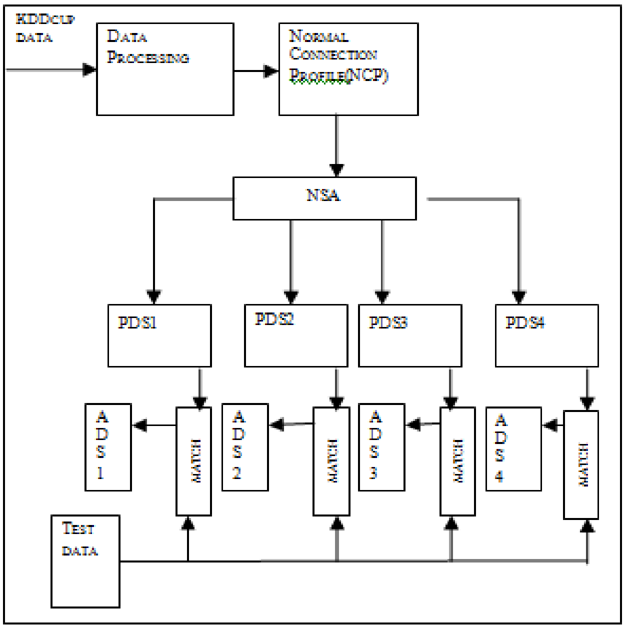

Fig 5.2 Detector generation using NSA

If any match is found then RS is not considered further else it is taken as potential detector.

### D. Active Detector Set Generation and Evaluation

In Figure 5.3, the method of evaluating ADS is shown. Only by this the performance and efficiency of the proposed approach can be seen using evaluation data set.

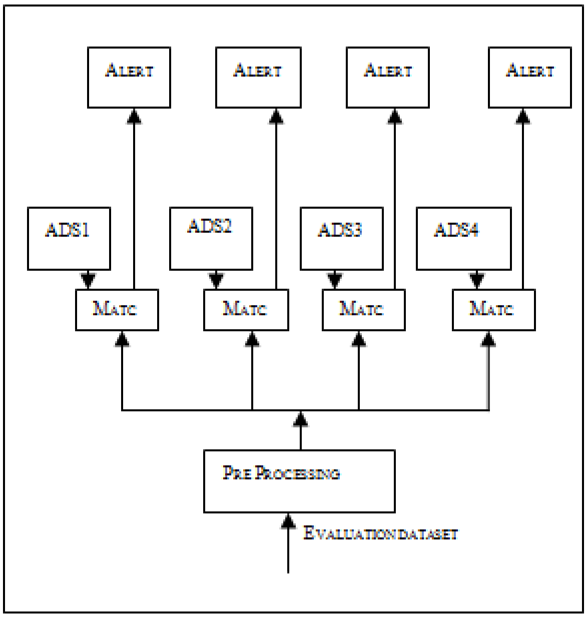

Fig 5.3 Evaluating Active Detector Set

In this the ADS set are evaluated using this data set. The detector that does not match with any of the abnormal connection is eliminated from the set. The number of abnormal connection matched with the instances in ADS will give the effectiveness of the detector set and the matched detector will be retained further.

The effectiveness of potential detector sets (PDS) generated can be found by evaluating it with abnormal data. If the generated potential detector set produces a good detection rate, then it is considered as the Active detector set. Evaluation of the PDS is as follows,

```
Initialise
    Matching Threshold (MT), Fitness (F), Abnormal
    Count (Acount), and Normal Count (Ncount).
Get Abnormal Data A
While PDS has next detector
    Get Detector D from PDS
    Match D and A
    If match found
    Increment F
End-While

If F>=MT
    A => Attack
    Acount++
Else
    A=> Normal
    Ncount++
Calculate Detection Rate
DR = Acount/(Acount+ Ncount)
```

The Matching Threshold here is user specified. If the given data need to be named as an 'Attack', then the fitness of that data must be greater than the MT. It means that the given data must get matched with MT number of or greater number of potential detectors.

For Example,
D = {00101, 10110,001100, 1010100, 110001}
A = 0111110101101010010010110110011 and
MT = 2

**10110** **00101**
0111110**1011010100100101**10110011
**1010100**

In the above example A's Fitness value = 3 because three elements from set D is matched with A. As Fitness is greater than MT here A is named as an Attack.

The Active Detector Set (ADS) generated is then used further to classify the test data. The set generated in this way is a static set. It can be made dynamic by producing new PDS in constant interval and updating the ADS with effective Detector set.

The above mentioned steps give normal flow between input and output of the proposed intrusion detection approach. By implementing these steps different sets of potential detector set are generated. The potential detector sets with higher detection rate are considered as the active detector set and is experimented with test data to observe the detection rate of unknown attacks.

## IV. RESULT AND EVALUATION

### A. *Experimental Results on Selected Feature*

In the initial phase of simulating the proposed approach, the NSL KDDcup dataset is pre processed using the tool Tanagra. In this the features of the dataset is reduced from 41 to 10. These 10 features are then experimented with the classification algorithm C4.5. This experiment is done to show that the selected features contributed more for higher detection rate and accuracy.

Scoring component that is included in Tanagra is used to compute score of a classification algorithm. In this experiment it is used to find the scores of C4.5 with all 41 features and with selected 10 features. Score gives the posterior probability of the positive class. Positive class here means the values of the class attribute (normal, Neptune, smurf etc.) in the KDD set. The result found is satisfactory by which it is understood that the selected 10 features contribute more to the attack detection. Table 2 provides the scores of C4.5 obtained with 41 features and selected 10 features.

TABLE II. COMPARISON OF C4.5 SCORE

| **Attack label** | **C4.5 score with 41 features** | **C4.5 score with 10 features** |
|---|---|---|
| Neptune | 0.998 | 0.997 |
| Warezclient | 0.954 | 0.967 |
| Ipsweep | 0.982 | 0.968 |
| Portsweep | 0.986 | 0.986 |
| Teardrop | 0.979 | 0.979 |
| Nmap | 0.980 | 0.980 |
| Satan | 0.971 | 0.962 |
| Smurf | 0.984 | 0.984 |
| Pod | 0.976 | 0.976 |
| Back | 0.978 | 0.978 |
| Guess_passwd | 0.975 | 0.975 |
| Multihop | 0.475 | 0.475 |
| Rootkit | 0.225 | 0.225 |
| Buffer_overflow | 0.975 | 0.975 |
| Imap | 0.975 | 0.975 |
| Warezmaster | 0.709 | 0.709 |
| Phf | 0.775 | 0.975 |
| Land | 0.075 | 0.075 |
| Spy | 0.425 | 0.425 |

From the table it is found that the score of C4.5 is nearly same both for 41 features and 10 features which means reducing the features does not influence the classifications.

This shows that right set of features have been chosen and hence C4.5 behaves similarly for the elaborate and reduced feature sets.

### B. *Experimental Results on Detector Sets*

#### 1) *Potential Detectors*

Considering a small subset of Normal Profile, Potential detector (PD) sets of different size are generated. On experimenting the Potential detector (PD) set upon Test data constituting only abnormal connection results, the following detection rate is obtained (see Table 3). This is done to check the impact of the size of Normal Profile and Potential Detector Set. It is found that as the size of normal profile and potential detector set increases the detection rate.

TABLE III. NP SIZE AND PDS SIZE IN IMPROVING DETECTION RATE.

| **Normal Profile small set of training data = 1468 Representation = 31 bit** | | | | |
|---|---|---|---|---|
| **Test Abnormal data = 9698 data** | | | | |
| NP = 100 | NP = 200 | NP = 300 | NP = 734 | NP = 1468 |
| PD = 50 | PD = 50 | PD = 50 | PD = 200 | PD = 200 |
| **Detection Rate** | | | | |
| 0.25 | 0.10 | 0.14 | 0.36 | 0.49 |
| 0.21 | 0.17 | 0.17 | 0.42 | 0.39 |
| 0.19 | 0.19 | 0.23 | *0.67* | *0.51* |
| 0.22 | 0.15 | 0.16 | 0.39 | 0.34 |
| 0.18 | 0.16 | 0.18 | 0.44 | 0.30 |

Potential Detector Set using 100% data of Normal Profile has been generated. Here all PDS is of size 200. The generated set is then verified for its effectiveness by making it to detect the abnormal data from a set of data – consisting of attacks that have been extracted from NSLKDD Train set. It contains 58630 number of attack data.

TABLE IV. POTENTIAL DETECTOR SETS AND ITS DETECTION RATE

| 100% of Normal Profile derived from NSLKDD Training data = 67,343 | Potential Detectors | Training Data2 Abnormal data from Training Set | Detection Rate |
|---|---|---|---|
| | PD1<br>No. of Detectors = 200 | | 70% |
| | PD2<br>No. of Detectors = 200 | | 58% |
| | PD3<br>No. of Detectors = 200 | | 66% |
| | PD4<br>No. of Detectors = 200 | | 72% |
| | PD5<br>No. of Detectors = 200 | | 55% |

Each set of Potential Detectors was able to produced detection rate of different range. Table 4 gives the details about it.

### C. *Active Detector Set*

The potential detector set that has produced detection rate above 50% is considered as the active detector set. Active Detector Set consists of 1000 detectors. Active Detector set is then used to detect the attacks in the NSL KDD Test Data. The result obtained using ADS is given in Table 5. The Active Detector Set is tested upon different sets of test data containing abnormal data alone. Here ten different sets are considered, starting from 10% percent data to 100% data. The total number of abnormal data found in the test data is 12,833.

Here matching threshold plays an important role. The result obtained is satisfactory. Even with MT =3, the active detectors were able to produce detection rate of 60% in average.

TABLE V. RESULT OBTAINED WITH ADS USING DIFFERENT MATCHING THRESHOLD

| Percent of Abnormal Data from NSL KDD data | Detection Rate MT=3 F>=3 | Detection Rate MT=2 F>=2 | Detection Rate MT=1 F>=1 |
|---|---|---|---|
| 10% | 59.46 | 80.04 | 95.87 |
| 20% | 60.34 | 80.52 | 96.26 |
| 30% | 60.7 | 80.29 | 95.92 |
| 40% | 61.15 | 80.61 | 95.81 |
| 50% | 61.38 | 81.07 | 96.04 |
| 60% | 61.44 | 81.01 | 96.03 |
| 70% | 61.37 | 80.92 | 95.97 |
| 80% | 61.12 | 80.70 | 95.95 |
| 90% | 61.08 | 80.69 | 95.93 |
| 100% | 61.2 | 80.70 | 95.80 |

## V. CONCLUSION AND FORESEEABLE ENHANCEMENTS

The focus of this project work is to identify significant features for intrusion detection and use negative selection algorithm to improve the anomaly based network intrusion detection in terms of detection rate and false positive rate. The Negative Selection Algorithm which is best suitable for anomaly based detection cannot produce good result with higher dimensional dataset like KDD cup99 dataset. To overcome this, the dimension of the KDD cup99 dataset is reduced to smaller size by selecting most relevant features and normal profiling is done using this reduced feature set. Using this normal profile different sets of potential detectors are generated. The potential detectors set that produced acceptable detection rate are carried to the active detector set. By this approach, a detection rate of 80 percent in average was able achieved with user defined matching threshold of 2 and a detection rate of 60 percent in average was achieved with user defined matching threshold of 3. This shows that the proposed approach works well with reduce set of features and Negative Selection Algorithm. Though certain tuning has been made to support NSA algorithm to improve detection rate of intrusion, certain improvements have to be still made. Some of the enhancements that could be made in future are as follows:

The enhancement to the methodology proposed can be made such that the false positive rate can be brought down that in turn improves the accuracy of the system. The features can be reduced according to specific attack types like DoS, Probe, U2R, R2L, thus making it possible to the system to indicate what type threat has occurred. Change can be made to the encoding technique used. Here binary encoding is done; instead real value encoding can be adopted which improves the effectiveness of the detectors so as to reduce false positive rate.

## REFERENCES

[1] Anup Goyal, Chetan Kumar, GA-NIDS: A Genetic Algotihm Base Network Intrusion Detection System.

[2] A. Chandrasekar, V.Vasudevan, P.Yogesh, Evolutionary Approach for Network Anomaly Detection Using Efective Classification. IJCSNS , VOL.9.No.1 Jan 2009

[3] Divyata Dal, Siby Abraham, Ajith Abraham, Sugata Sanyal, Mukund Sanglikar, Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System, Computer Information Systems and Industrial Management Applications, 2008. CISIM '08. 7th

[4] F. Gu, J. Greensmith and U. Aickelin (2008): 'Further Exploration of the Dendritic Cell Algorithm', 7th International Conference on Artificial Immune Systems (ICARIS 2007), pp 142-153, Phuket, Thailand, Springer LNCS 5132.

[5] H.Gunes Kayacik, A. Nur Zincir-Heywood, Malcolm I.Heywood, Selecting Features for Intrusion Detection: A feature Relevance Analysis on KDD 99 Intrusion Detection Datasets.

[6] Jamie Twycross and Uwe Aickelin, Biological Inspiration for Artificial Immune Systems.

[7] Jing Tao Yao, Songlun Zhoa and Lisa Fan, An Enhanced Support Vector Machine Model for Intrusion Detection.

[8] Jiong Zhang and Mohammad Zulkernine, Network Intrusion Detection using Random Forrest.

[9] Kamran Shafi, Hussein A.Abbass, Biologically-inspired Complex Adaptive Systems Approaches to Network Intrusion Detection, Science Direct, Information Security Technical Report, 2007.

[10] Ming-Yang Su, Gwo-Jong Yu, Chun-Yuen Lin, A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach, Science Direct, Computer Security, 2009

[11] Muhammed Awais Shibli, Jeffy Mwakalinga and Sead Muftic, MagicNET: The Human Immune System and Network Security System, IJCSNS, Vol. 9, No.1, Jan 2009.

[12] Neveen I. Ghali, *Feature Selection for Effective Anomaly-Based Intrusion Detection,* IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009

[13] Norbik Bashsh, Idris Bharanidharan Shanmugam, Abdul Manan Ahmed, *Hybrid Intelligent Intrusion Detection System*, World Academy of Science, Engineering and Technology 11 2005.

[14] R. Geetha Ramani, M.Uma Maheswari, G.Gayathri, *Attackers In Networks*, Proceedings of the 5th Annual Conference on Information Science, Technology and Management, 2007.

[15] Sabine Bachmayer, *Artificial Immune System*, Manuscript, 2007.

[16] Shelly Xiaonan Wu* Wolfgang Banzhaf, *The Use of Computational Intelligence in IntrusionDetection Systems: A Review*, Technical Report 2008-05, Memorial University of Newfoundland

[17] Steven A.Hofmeyr and Stephanie Forrest, *Immunity by Design: An Artificial Immune System.*

[18] Srilatha Chebrolu, Ajith Abraham and Johnson P Thomas, Hybrid Feature Selection for Modeling Inntrusion Detection System.

[19] Srinivas Mukkamala , Andrew H. Sung, Feature Selection for Intrusion Detection using Neural Networks and Support Vector Machines

[20] Su-Yun Wu, Ester Yen, Data mining-based intrusion detectors, Elsevier, Expert System with Applications, 2009.

[21] Wafa S. Al-Sharafat, Reyadh Sh.Naoum, Adaptive Framework for Network Intrusion Detection by Using Genetic- Based Machine Learning, IJCSNS Vol. 9, No. 4, Apr. 2009.

[22] Yang Li, Jun-Li Wang, Zhi-Hong Tian, Tian-Bo Lu, Chen Young, Building lightweight intrusion detection system using wrapper-based feature selection mechanisms. Science Direct Computer and Security, 2009.

[23] 23. Zhongxue Yang, Adem Karahoca, Ning Yang, Nizamettin Aydin, Network Intrusion by Using Cellular Neural Network with Tabu Search, IEEE Computer Society, Bio-Inspired, Learning and Intelligent System for Security, IEEE 2008.

[24] Zorana Bankovic, Jose M.Moya, Alvaro Araujo, Slobodan Bojanic and Octavio Nieto- Taladriz, A Genetic Algorithm-based Solution for Intrusion Detection, Journal of Information Assurance and Security 4(2009) 192-199,

[25] Jothi Lakshmi U, S.Sivasathya, " Significant Feature Set Identification for Network Intrusion Detection, Proceeding of the International Conference on Advanced Computing and Communication,(ICACC 2010),Page Number – 158-162, May 3-4, Kanjirapally, Kerala, India..

[26] www.wikipedia.org

[27] www.windowsecurity.com

[28] www.idstutorial.com

[29] www.vdetector.zhouji.net

[30] KDDcup1999: http://kdd.ics.uci.edu/dataset/kddcup99/kddcup99.html

[31] www.timberlinetechnologies.com

[32] www.snort.org

[33] www.cisco.com